CHAPTER 6. Notes

This section contains acronyms, abbreviations and a list of terms and definitions needed to understand this document.

6.1 Acronyms and Abbreviations

AC	Access Control
ACCS	Army Command and Control Systems
ACK	Acknowledgment
ACP	Allied Communications Publication
ADPE	Automatic Data Processing Equipment
AE	Authentication Exchange
AGCCS	Army Global Command and Control System
AIG	Address Indicator Group
AIS	Automated Information System
AITS	Adopted Information Technology Standards
AIX	Advanced Interactive eXecutive
AMHS	Automated Message Handling System
ANSI	American National Standards Institute
API	Application Programming Interface
APP	Application Portability Profile
APSE	Ada Programming Support Environment
ASC	American Standards Committee
ASCII	American Standard Code Information Interchange
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASRD	AWIS Software Requirements Specification Document
ASSET	Asset Source for Software
ATCCS	Army Tactical Command and Control Systems
ATM	Asynchronous Transfer Mode
AUTODIN	Automated Data Information Network
AWIS	Army WWMCCS Information System
BLOB	Binary Large Object
BMP	Bitmapped picture
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
CAD	Computer-Aided Design
CASE	Computer-Aided Software Engineering (See ISEE)
CASS	Common ACCS Support Software
CCB	Configuration Control Board
CCIP	Command Center Initiatives Program
CCITT	Consultative Committee on International Telegraph and Telephone
CDA	Computer Design Activity
CFA	Center for Architecture
CFE	Center for Engineering
CFII	Center for Integration & Interoperability
CFS	Center for Standards
CHS	Common Hardware Software
CIM	Corporate Information Management
CINC	Commander-in-Chief
CJCS	Chairman of the Joint Chiefs of Staff
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLI	Client Library Interface

CLNP	Connectionless Network Protocol
CM	Configuration Manager
CMIS/P	Common Management Information Services and Protocols
CMW	Compartmented Mode Workstation
CN	Communications Network
COE	Common Operating Environment
CONUS	Continental United States
CORBA	Common Object Request Broker Architecture
COTS	Commercial-Off-The-Shelf
CRT	Cathode Ray Tube
CSE-SS	Client Server Environment System Services
CTE	Center for Test and Evaluation
CTOS	Convergent Technologies Operating Systems
CTT	Commander's Tactical Terminal
DA	Data Administrator
	Data Access
DAA	Designated Approving Authorities
DAC	Discretionary Access Control
DAPM	Domain Analysis Process Model
DAPMO	Data Administration Program Management Office
DARIC	Defense Automation Resources Information Center
DAS	Data Access Service
DASD (IM)	Deputy Assistant Secretary of Defense for Information Management
DBA	Database Administration
DBIF	Database Interface
DBMS	Database Management System
DBs	Databases
DBWG	Database Working Group
DCE	Distributed Computing Environment
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DDI	Director of Defense Information
DDL	Data Definition Language
DDS	Data Distribution System
DEPSECDEF	Deputy Secretary of Defense
DES	Data Encryption Standard
DGSA	Defense Goal Security Architecture
DI	Date Integrity
DIA	Defense Intelligence Agency
DID	Data Item Description
DII	Defense Information Infrastructure
DIS	Defense Information System
DISA	Defense Information Systems Agency
DISC	Defense Information System Council
DISN	Defense Integrated Services Network
DISSP	Defense Information System Security Program
DITPRO	Defense Information Technical Procurement Office
DMF	Data Management Facility
DML	Data Manipulation Language
DMRD	Defense Management Review Decision
DMS	Defense Message System
DNS	Domain Name Server
DNSIX	DODIIS Network Security for Information Exchange
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction

DODIIS	Department of Defense Intelligence Information System
DODM	DoD Manual
DS	Digital Signature
DSN	Defense Switched Network
DSRS	Defense Software Repository System
DSS	Digital Signature Standard
DSSSL	Document Style Semantics and Specification Language
DTD	Document Type Definition
DTG	Date-Time-Group
DTLS	Descriptive Top-Level Specification
DTMP	Data Communications Protocol Standards Technical Management Panel
E	Encipherment
EAD	Executive Agent Developer
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce, and Transportation
EEI	External Environment Interface
E-mail	Electronic Mail
E.O.	Executive Order
EPLRS	Enhanced Position Location Reporting System
ES	End System
FAPM	Functional Activity Program Manager
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FIPS PUB	Federal Information Processing Standards Publication
FMWG	File Management Working Group
FOC	Full Operational Capability
FTP	File Transfer Protocol
FY	Fiscal Year
GBS	Global Broadcast System
GCCS	Global Command and Control System
GCSS	Global Command Support System
GNMP	Government Network Management Profile
GOSIP	Government Open System Interconnection Profile
GOTS	Government-Off-The-Shelf
GUI	Graphical User Interface
HCI	Human Computer Interface
HP	Hewlett-Packard
HP-UX	Hewlett Packard UNIX Operating System
HTML	Hypertext Markup Language
HYTIME	Hypermedia/Time-Based Structuring Language
I&A	Identification and Authentication
IAW	in accordance with
ICASE	Integrated Computer Aided Software Engineering
ICCCM	Inter-Client Communications Conventions Manual
ID	Identification Identifier
IDD	Interface Design Document
IDS	Interface Design Specification
IEEE	Institute of Electrical and Electronic Engineers
IEMATS	
IETM	Interactive Electronic Technical Manual
I/F	Interface

IGES	Initial Graphics Exchange Specification
IGOSS	Industry/Government Open System Specification
IM	Information Management
IMS	Information Management System
INCA	Intelligence Communications Architecture
INRI	International Research Institute
INX	Information Exchange
I/O	Input/Output
IP	Internet Protocol Internetwork Protocol
IRAC	International Requirements and Design Criteria
IRDS	Information Resource Dictionary System
IRS	Interface Requirements Specification
I&RTS	Integration and Runtime Specification
IS	Information System
ISA	Information System Architecture
ISB	Intelligence Systems Board
ISDN	Integrated Services Digital Network
ISEE	Integrated Software Engineering Environment
ISO	International Standards Organization
IT	Information Transfer
ITPB	Information Technology Policy Board
ITRUS	Information technology reuse
ITSG	Information Technology Standards Guidance
JANAP	Joint Army, Navy, Air Force Publication
JCS	Joint Chief of Staff
JIEO	Joint Interoperability and Engineering Organization
JMCIS	Joint Maritime Command Information System
JMF	Joint Message Format
JOBES	Joint Operation Planning and Execution System
JOTS	Joint Operation Tactical System
JTC	Joint Technical Committee
JTC3A	Joint Tactical Command, Control and Communications Agency
JTT	Joint Tactical Terminal
JVMF	Joint Variable Message Format
LAN	Local Area Network
LAPB	Link Access Protocol B
LCM	Life Cycle Management Life Cycle Model
LDMX	Local Digital Message Switch
LSE	Local Subscriber Environment
MAC	Mandatory Access Control
MATT	Multimission Advanced Tactical Terminal
Mbs	Megabytes
MCG&I	Mapping, Charting, Geodesy and Imagery
MHS	Message Handling System
MIL-STD	Military Standard
MIS	Management Information Systems
MLS	Multilevel Security ulti-level Secure
MOA	Memorandum of Agreement
MS	Management Services
MSB	Most Significant Bit

N	Notarization
NACK	Negative Acknowledgment
NATO	North Atlantic Treaty Organization
NCA	National Command Authority
NCCS	Navy Command and Control System
NCCOSC	Navy Command, Control and Ocean Surveillance Center
NCSC	National Computer Security Center
NDI	Non-Development Items
NIST	National Institute of Standards and Technology
NLSP	Network Layer Security Protocol
NM	Node Management
NRaD	Navy Command, Control and Ocean Surveillance Center Research and Development
NSA	National Security Agency
NSD	National Security Directive
NSRD	National Software Reuse Directory
NTIS	National Technical Information Service
NVLAP	National Voluntary Laboratory Accreditation Program
OASD	Office for the Assistant Secretary of Defense
ODA	Office Document Architecture
ODIF	Office Document Interchange Format
ODL	Office Document Language
ODM	Organizational Domain Modeling
OIW	OSI Implementors' Workshop
OMB	Office of Management and Budget
OODBMS	Object-Oriented Database Management System
ORB	Object Request Broker
OS	Operating System
OSD	Office of the Secretary of Defense
OSE	Open System Environment
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OTCIXS	Officer-in-Tactical-Command Information Interchange System
OTH-T	Over-The-Horizon Targeting
OTI	Office of Technical Integration
PCIS	Portable Common Interface Set
PCTE	Portable Common Tools Environment
PDES	Product Data Exchange using STEP
PEX	PHIGS Extension to X Windows
PHIGS	Programmer's Hierarchical Interactive Graphics System
PLA	Plain Language Addressee
PLRS	Position Location Reporting System
PMP	Program Management Plan
POSIT	
POSIX	Portable Operating System Interface for Computer Environments
PSA	Principal Staff Assistant
PSDS	Public Switched Data Service
RC	Routing Control
RDA	Remote Database Access
RDBMS	Relational Database Management System
RI	Routing Indicator
RISC	Reduced Instruction Set Computer
RLF	Reuse Library Framework
ROAMS	Reusable Object Access and Management System
ROM	Read Only Memory

RPC	Remote Procedure Call
RS	Relay System
RTF	Rich Text Format
SAGD	Security Architecture and Guidance Document
SAME	SQL Ada Module Extensions
SAMeDL	SQL Ada Module Extension Description Language
SAMP	Security Association Management Protocol
SBIS	Sustaining Base Information Architecture Framework
SCSI	Small Computer System Interface
SDD	System Design Document
SDNS	Secure Data Network System
SECDEF	Secretary of Defense
SFUG	Security Features User's Guide
SGML	Standard Generalized Markup Language
SII	System Internal Interfaces
SIPRNET	Secret Internet Protocol Router Network
SMFA	System Management Functional Areas
SMM	Systems Management Manual
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SRI	Standing Request for Information
SRS	Software Requirements Specification
SSDD	Support Software Design Document
STACCS	Standard Theater Army Command And Control System
STARS	Software Technology for Adaptable Reliable Systems
STD	Standard
STEP	Standard for the Exchange of Product Model Data
STM	Synchronous Transfer Mode
S/W	Software
SWG	Security Working Group Special Working Group
TA	Technical Architecture
TADIL	Tactical Data Link
TADIXS	Tactical Data Interchange System
TAFIM	Technical Architecture Framework for Information Management
TBD	To Be Determined
TBS	To Be Specified
TCIM	Tactical Communications Interface Module
TCIS	TCIM Common Interface Software
TCP	Transport Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDI	Trusted Database Interpretation
TFA	Transparent File Access
TFM	Trusted Facility Manual
TIBS	Tactical Information Broadcast Service
TIM	Technical Integration Manager
TLSP	Transport Layer Security Protocol
TNI	Trusted Network Interpretation
TP	Traffic Padding
TRE	Tactical Receiving Equipment
TRM	Technical Reference Model
TRI-TAC	Tri-Service Tactical Communications Systems
TSIG	Trusted Systems Interoperability Group

UDP	
UI	UNIX International
UIDL	User Interface Definition Language
UIMS	User Interface Management System
UISRM	User Interface System Reference Model
UserID	User Identifier
USMTF	United States Message Text Format
VME	
VMF	Variable Message Format
WAN	Wide Area Network
WWMCCS	World-Wide Military Command and Control System
X	X Windows System

6.2 Glossary

The following list identifies the terms that are used in this document along with their associated meanings.

Abstract Syntax Notation One (ASN.1)
An abstract syntax can be thought of as a named group of types. ASN.1 is a flexible yet standard method of describing data structures for representation, encoding, transmission and decoding. ASN.1 provides a set of formal rules for describing the structure of objects independently of machine-specific encoding techniques.

access
A specific type of interaction between a subject and an object resulting in the flow of information from one to the other.

access control
The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.

access rights
The set of types of interaction between subjects and an object resulting in the flow of information from one to the other (e.g., owner-read and execute; group-read; others-none).

Account Group
Account Groups are a set of logically related system functions provided by one or more COE segments. COE segments may provide system functions for one or more account groups

accountability
The property that enables activities on a system to be traced to individuals who may be held responsible for their actions.

Accounting management (AM)
AM is one of the five major Systems Management Functional Areas (SMFAs) that is described in the ISO OSI Management Framework and System Management Overview standards. The AM SMFA defines requirements to enable identification or negotiation of mechanisms for associating and collecting system resource usage charges, to initiate or deactivate charging algorithms, and to monitor or to report account relevant information.

Administrative Domain
The set of computing platforms and their associated resources (e.g., users, profiles, segments) that are under the administrative control of a single entity

administrative domain
The set of computing platforms and their associated resources (e.g., users, profiles, segments) that are under the administrative control of a single entity.

Application

An application is an executable program that can be launched from a desktop icon.

Association Control Service Element (ACSE)

The ACSE provides essential services for applications related to connection establishment, connection termination, and connection aborting. One of the parameters used by ACSE to identify the particular application to which an association is to be established is the Application Entity (AE) title.

assurance

A measure of confidence that the security features and architecture of the COE accurately mediate and enforce the security policy

Attribute

An attribute is a property of a managed object and has a value. Mandatory initial values for attributes can be specified as part of the managed object class definition. Attributes are grouped into mandatory and conditional packages.

audit trail

A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a transaction from its inception to final results.

Automatically

Indicates processing initiated during execution of other processes, but dependent on information and/or parameters to be generated or supplied to these other processes. The information / parameters may be data dependent, or application dependent, or dependent on a manual process/human intervention. It will include controls qualifying the processing involved.

availability

The state when data is in the place needed by the user, at the time the user needs them, and in the form needed by the user

classification

A term that represents the hierarchical portion of the security level.

Cognizant Technical Official (CTO)

The CTO is the person responsible for the technical requirements related to the source selection process. (*Federal Acquisition Regulation, Apr 1990*). If no CTO is appointed, the term "Acquisition Authority" should be used in this document.

Commit/Rollback

An individual transaction is processed (commit) or discarded (rollback) by the proponent maintainer of the data items involved.

Common management information services and common management information protocol (CMIS/CMIP)

CMIS and CMIP are the services and protocol developed by ISO for OSI systems management. CMIP is the protocol used by an application process to exchange information and commands for the purpose of remotely managing computer and communication resources, while CMIS specifies the service interface to CMIP. CMIS/CMIP may be used over a variety of underlying protocol stacks, including full-stack OSI, a mixed upper layer OSI over TCP/IP, and just the IEEE lower layer stack (LLC and below). In the former case, in order to transfer management information between open systems using CMIS/CMIP, peer connections (associations) must be established. This transfer requires the establishment of an application association, a session connection, a transport connection, and, depending upon the underlying communications technology, network and link connections.

confidentiality

The concept of protecting data from unauthorized disclosure.

Configuration management (CM)

CM is one of the five major SMFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The CM SMFA defines requirements to determine/monitor (via interrogation, polling or event-driven reporting), to detect changes in, and to control the arrangement, relationships, characteristics and state (for example, initialize/terminate,

activate/deactivate, idle/busy, etc.) of individual and specifiable aggregates of managed resources so as to maintain continuous operation and/or delivery of service. CM as used in this MIL-HDBK is not to be confused with CM as used in MIL-STD-483 (*Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs*) or MIL-STD-1456 (*Configuration Management Plan*).

Databases

Databases are archival repositories persistently stored on electro/optical media. Databases are accessed or updated by database management systems. Databases are generally used by, and shared among, manager systems by means of standard database query languages, such as SQL and RDA. Some databases may be integrated across several different manager systems and/or management domains.

deadman function

A capability that locks or makes inoperable the user's terminal or workstation if the user does not use the input devices (e.g., keyboard, mouse, trackball) for a configurable time period.

Directory services

The Directory Services (IS 9594, CCITT X.500) is an application service which enables users to query on the names of other users (for example, message recipients, applications, hosts names) and to obtain additional network information (for example, originator/recipient addresses, application entity titles, Presentation Service Access Point (PSAP) of application entities, network address of host computers).

discretionary access control

A means of restricting access to objects based upon the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

DoD Trusted Computer System Evaluation Criteria (TCSEC)

A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is Government Standard DoD 5200.28-STD and is frequently referred to as "The Criteria" or "The Orange Book."

Domains

Domains represent different ways of aggregating and distributing management authority and/or management scope for any specific reason. Often, large, complex aggregations of resources are partitioned into domains to make the inherent complexity manageable. An illustrative domain partitioning is between telecommunications service providers and their service users. The provider domain consists of the provider-owned physical and logical resources that make up the provider's network. The user domain consists of the user-owned resources that comprise the user's private network. The services obtained from the provider domain may or may not be considered to be in the user's domain, while the resources that underlie these services are definitely not in the user's domain.

Dynamically Generated Processing

Indicates processing initiated during execution of other processes, but dependent upon information and/or parameters to be generated or supplied to these other processes. The information/parameters may be data dependent, or application dependent, or dependent on a manual process/human intervention. It will include controls qualifying the processing involved.

Element manager system

An element manager system manages the resources specific to a particular component class of a distributed system; for example, a bridge manager is an element manager system that manages LAN bridges.

Enterprise management

Enterprise management is the management of the aggregate of all systems and networks within an organization or enterprise.

Event

An event is any occurrence that changes the status of a managed object. The event may be spontaneous or planned, persistent or temporary, and may trigger other events or be triggered by other events.

Fault management (FM)

FM is one of the five major SMFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The FM SMFA defines requirements to define, detect, identify, monitor, isolate the causes of, log, analyze, test for, trace and correct problems in abnormal or disabled managed resources.

Hot Backups

Hot backups are fully configured sites which can take over all the functions of the primary site they are backing up. They are set up to come on-line within a short time after the primary site fails.

Human engineering

Human engineering is the consistent presentation of management information from heterogeneous network resources (for example, help screens, summarized data, graphical user interfaces, ergonomics, etc.). The use of human engineering will enable the network manager to quickly and easily comprehend the NM system's capabilities, to use the NM functions efficiently, and to allow flexibility in performing the desired operations.

identification and authentication

The combination of a process that enables recognition of an entity by a system, generally by the use of unique machine-readable names (identification) and the verification of the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system (authentication).

integrity

The degree of protection for data from intentional or unintentional alteration or misuse.

least privilege

The principle that requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

manage

The act of configuring, administering, operating and maintaining the COE security requirements.

Managed Object

ISO Reference

Managed object

Managed objects are abstract representations of resources in a network. A managed object may represent a physical entity, a network service, or an abstraction of a resource which exists independently of its use in management. Managed object definitions of OSI resources, a critical requirement for interoperable NM systems, are beginning to be standardized. IS 10165-4 contains a set of standard guidelines for the definition of managed objects. IS 10165-2 and a number of the ISO/IEC 10164 series of standards contain definitions of common management information that can be imported into definitions of managed objects. Due to the importance of managed object definitions, many standards groups, vendors and user consortia (for example, CCITT, the IEEE 802, the NMF and the OIW (Open Systems Environment Implementors Workshop) NM Special Interest Group) are defining managed objects. The DoD has been active in defining military-unique managed objects. Specifically, MIL-STD-2204, SAFENET, defines a number of managed objects which are used to support the synchronization of distributed clocks in a tactical shipboard local area network.

Managed system

Managed systems contain agent processes that act on behalf of, and therefore interact with, remote manager systems or managed resources. The agent processes interact directly with the managed objects that characterize the managed resources. A single object may represent one or many resources, and a single resource may be characterized by one or many objects (each providing different management views of the actual resource). Such managed systems are often embedded in the hardware and/or software of the resource to be managed.

Management domain

A management domain is a set of managed objects which is accessible from a single management authority. For instance, a key management center may be associated with a key management domain.

Within a security domain, however, a key management domain, an access control domain, and an audit management domain must overlap.

Management gateways

Management gateways translate and map between different management communication protocols, services, and/or different styles of representing the management information associated with specific resources. Such differences typically arise between (a) manager systems, such as n-layer managers or element managers, and (b) manager systems that manage an entire system. Differences also arise between managers of entire, but different, systems, such as managers of different protocol stacks. Management gateways can be used to accommodate management of existing, legacy resources. Management gateways can also be used to accommodate management of other future resources.

Management information base (MIB)

A MIB is a distributed repository of the management information that represents the resources being managed. MIBs are also run-time, real-time repositories available to be shared among manager systems, managed systems, and management gateways by means of standard management communication protocols. Many types of MIBs exist.

Manager system

A manager system is the hardware and software entity which receives management inputs from local operators, receives management inputs (such as spontaneous management-related notifications) from agent processes in remote manager systems (or in remote managed systems) and/or initiates requests for management information from agents in remote manager systems or in remote managed systems. (Management communications with remote manager systems or managed systems may occur via a standard, general purpose management communications protocol, such as CMIP.) A manager system can make management decisions via supported management applications. A manager system can effect decisions and other management operations either locally on local managed objects or remotely to manager systems or to managed systems representing remote managed objects.

Mandatory Access Control (MAC)

mediates access to an object based on the clearance level of the subject (user) and the sensitivity label of the object. (These controls are always enforced above any discretionary control implemented by users).

markings

Markings are human-readable labels presented on computer screens, printed on paper or affixed to removable media that describe the sensitivity of the information presented as to its classification, caveats, and handling restrictions or provide warnings to users in compliance with federal laws and regulations.

mechanism

A capability which must be properly managed in order to enforce the COE security requirements.

message data

TBS.

Mirrored Databases

Replication and maintenance of a database on a transaction basis for the purpose of rapid error or failure recovery as supported by the resident COTS RDBMS own system utilities and operating system.

mode of operation

A description of the conditions under which an AIS functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users.

multi-level secure

A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.

multi-level secure mode of operation

A mode of operation where all of the following statements are satisfied about each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts:

a. Some do not have valid personnel clearance for all the information processed in the AIS.

b. ll have the proper clearance and have the appropriate formal access approval for that information to which he/she is to have access.

c. ll have a valid need-to-know for that information to which they are to have access.

Multimedia

The Interactive Multimedia Association defines multimedia as "two or more media types (audio, video, imagery, text, and data) electronically manipulated, integrated, and reconstructed in synchrony".

N-layer manager

An n-layer manager is a manager that manages the resources specific to one layer of a stack of networking protocols. Such managers often do not use general purpose management communication protocols (for example, CMIP), services and management information. Rather, they often use mechanisms and/or services specific to the protocol layer being managed.

Network

A network is a connected set of switching and transmission communication components. The network includes all hardware and software communications components residing in such switching and transmission components, as well as in end-systems, such as computers, that are attached to the network.

Network administrator

A network administrator is the person responsible for operating a NM system.

Network Control Center (NCC)

An NCC is the top-level DoD NM entity within a management domain. The NCC coordinates and controls NM functions within a domain and between domains.

Network management (NM)

NM is the set of activities to bring up and establish networking resources, keep them operational, fine tune their operation, account for their usage, and support their protection from unauthorized use and tampering. Typically, the term is also used to refer to such management activities as well as a myriad of other management functions and activities, of greater or lesser scope, when any of such management functions and activities are applied to other kinds of manageable resources besides telecommunications (voice), messaging, video and computer communications networks. Such other management functions and activities may be associated with the early planning stages, growth and retirement of resources, as well as with daily operation and utilization. Such other resources may include general purpose information processing resources such as computers, their system software/peripherals, the distributed multimedia applications they host, or the aggregate of all such resources together with the networking resources used to interconnect them.

Network management system (NM system)

An NM system is the aggregate of the operational and administrative mechanisms, protocols, procedures and tools to provide NM. The NM system may consist of manager systems, managed systems, and management gateways.

Network manager

A network manager is a specialized manager system (see above) used to manage networking resources.

non-repudiation.

The proof of delivery or origin of information transactions.

object

A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Package

A package is a term used in the definition of OSI managed objects. A package refers to a collection of attributes, notifications, operations, and/or behaviors which are treated as a single module in the specification of a managed object class. Packages may be specified as being mandatory or conditional when referenced in a managed object class definition. However, the provision of options in managed object class definitions is discouraged on the grounds that internetworking becomes more difficult as the number of conditional packages increases.

password

(1) A protected/private character string used to authenticate an identity.

(2) A discretionary access control mechanism that represents the access control matrix by row by attaching passwords to protected objects.

Performance management (PM)

PM is one of the five major SMFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The PM SMFA defines requirements to provide the attributes, services, and event reports to measure, estimate, monitor (via interrogation, polling or event driven reporting), track, store, analyze/evaluate, maintain and otherwise control the configuration, operational characteristics, performance/effectiveness characteristics, performance measuring/monitoring characteristics, performance tuning characteristics, performance testing characteristics and/or quality-of-service characteristics and objectives (for example, responsiveness, availability, utilization, and residual capacity) associated with individual managed resources or specifiable aggregates of managed resources.

Profile

A profile defines the user configuration or a subset thereof contained within an account group. User configuration encompasses the definition of icons, menu structure, group membership, and environmental variables needed to successfully execute the system function within an account group. A master profile exists for each account group and contains the user configuration for all of the system functions in the account group.

Note: A user is assigned one or more profiles based on the systems functions the user will need to perform his/her functional activities.

Proponent Scheme

Describes the sites at which databases are replicated and also who owns and has update authority with respect to the data at each site. It refers to proponency at the source and record level.

purge

The removal of sensitive data from an Automated Information System (AIS), AIS storage device, or peripheral device with storage capacity, at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. After a purge, the medium can be declassified by observing the review procedures of the respective agency.

read access

A fundamental operation that results only in the flow of information from an object to a subject.

Remote Operations Service Element (ROSE) protocol

ROSE provides remote operation capabilities, allowing request/response interaction between entities of a distributed application. That is, upon receiving a remote operation request from one entity, the receiving entity attempts to perform the requested operation and reports the outcome of the attempt to the requesting entity.

Replication Scheme

Information that precisely identifies DBs, or partitions of DBs, to be copied and/or distributed, replication schedules, and master/remote sites that are to receive the copies.

Router

A router is a device that provides the network layer relay function connecting two subnetworks. That is, the device receives data from one network entity and forwards it to another network entity.

roles

The assignment of a user to a specific functionality within a system or application.

Security domain

A security domain is a set of entities that is subject to a single security policy and administered by a single authority. The entities within a particular security domain may be related to a functional or geographic area. A security domain relates to a collection of security devices and their management centers. A particular security device may operate within more than one security domain. In this case, exact rules must exist to regulate which security policy to follow for each instance of communications.

security level

The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security management (SM)

SM is one of the five major SMFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The SM SMFA defines requirements to support combat of threats by identifying and logging users of sensitive resources, monitoring usage of sensitive resources, defining, identifying, and monitoring security-relevant events, creating, and analyzing audit trails of such events, users and usage, controlling certain aspects of security services and mechanisms (for example, initiating re-keying or algorithm re-initialization), and controlling configuration (for example, isolating infected resources or denying/limiting resource access to unauthorized applications, users, or their requests).

security policy

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

security-relevant event

Any event that attempts to change the security state of the system, (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.,). Also, any event that attempts to violate the security policy of the system, (e.g., too many attempts to login, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.).

security requirements

The types and level of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

sensitivity labels

A piece of information that represents the security level of an object. Sensitivity labels are used by the COE Security Services as the basis for mandatory access control decisions.

Session

The implementation of the user's profile(s) within the user's work environment from login to logout. The session provides the resources that the user needs to perform the functions included in the user's profile(s).

Spatial DBMS

Geographic information system that organizes and maintains spatial data (i.e. data with graphical attributes) in terms of type, scale, location(s), extent, topology and geometry. Supports queries of spatial data where the selection criteria are defined by spatial attributes.

Specific management functional area (SMFA)

ISO has partitioned systems management into five SMFAs to categorize requirements for the support of systems management. The five SMFAs are: configuration management, fault management, performance management, security management, and accounting management. System Management Function standards (see para 3.2.35) define management services/capabilities to meet these requirements. In some cases, different SMFAs have the same requirements and therefore use the same SMFs to satisfy the common requirements.

SRI

A Standing Request For Information (SRI) is a capability in which CASS monitors for the occurrence of conditions established by an application program, and notifies the calling or establishing application program when the conditions are satisfied. An SRI may be one of three types: timer-based, data-based, or message-based.

subject

An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

System

A system is a set of information processing and data processing resources (such as computers), together with any supporting system software (such as operating systems and DBMSs), any peripheral devices, any supported applications and files, and any communications infrastructure that interconnects the system's components, end-users of such system resources, and the users and components of other systems. A system is generally considered to include all hardware and software components, facilities, personnel, and procedures which are necessary to support applications.

System Function

A system function is an executable program or function within the program that may be represented by an icon on the desktop or a menu item in the menuing structure. A COE segment provides one or more system functions. An application or a separable function within an application is a system function.

system high mode of operation

A mode of operation where all of the following statements are satisfied about each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

a. A valid personnel clearance for all information on the AIS.

b. Formal access approval for, and has signed nondisclosure agreements for all the information to which he/she is to have access.

c. A valid need-to-know for that information to which he/she is to have access.

system resources

Those entities that belong to and are controlled by the system.

Systems management

Systems management is the set of activities to bring up and establish system resources, keep them operational, fine tune their operation, account for their usage, and support their protection from unauthorized use and tampering. Typically, as with the term *network management*, the term *systems management* is also used to refer to a myriad of other management functions and activities, of greater or lesser scope, which may also be applied to the management of resources other than system resources.

Systems Management Function (SMF)

The SMFs include functions such as object management, state management, alarm reporting, event report management, log control, security alarm reporting, and accounting meter. The many parts of ISO/IEC 10164, are the SMF standards that define specific services, notifications (events), and/or attributes to support different NM requirements.

Transaction Journalling

Individual messages or database transactions are stored in a journal file, which may be a linear log file or a circular file.

trusted path

A mechanism by which a person at a terminal or workstation can communicate directly with the security services of the COE. This mechanism can only be activated by the person or the security services and cannot be imitated by untrusted software.

Trusted Role

A trusted role is a profile in which the system functions assigned to that profile may affect the implementation of the security policy within the system.

trusted users

Those users that have administrative responsibilities for the system that require the use of privileged commands to perform their duties (e.g., security officer, systems administrator).

user

Any person who interacts directly with a computer system.

write

A fundamental operation that results only in the flow of information from a subject to an object.

write access

Permission to write to an object.